

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-6. (Cancelled)

7. (Currently Amended) A method for allowing a client application to establish, in a client network, a first connection having a first security level, with a first port of a server application hosted in a server machine linked to a server network, in order to send messages addressed to the server machine, said messages passing from the client network to the server network through a network layer (CR) of a gateway machine, comprising:

creating a second port in the gateway machine;

ordering the network layer (CR) of the gateway machine to reroute to the second port of the gateway machine any message sent and addressed to the first port of the server application, addressed to the server machine;

receiving at the second port of the gateway machine a request addressed to the first port of the server application to establish said first connection with the first port of the server application;

listening to the second port of the gateway machine to detect ~~a~~the request addressed to the first port of the server application to establish said first connection with the first port of the server application; and[[;]]

generating, in the gateway machine, a thread for establishing said first connection when a the request to establish said first connection is detected in the second port of the gateway machine.

8. (Previously Presented) A method according to claim 7, further comprising:
defining a third port of the server application for receiving at least one of the messages with a second security level; and whereas said thread comprises;
establishing said first connection in a first phase with a first security level in a first interface associated with the second port and with said request;
establishing in a second phase a second connection with a second level of security in a second interface to the third port in the server machine;
writing with the second security level in the second interface any message read in the first interface with the first security level in a third phase, and;
writing with the first security level in the first interface any message read in the second interface with the second security level in a fourth phase.

9. (Previously Presented) A method according to claim 8, further comprising:
ordering the network layer (CR) of the gateway machine to delete any message sent to the third port.

10. (Previously Presented) A method according to claim 7, wherein the steps of creating and ordering are executed automatically by a first process of the gateway machine and in that said first process generates a second process that executes the third and the fourth step.

11. (Previously Presented) A method according to claim 8, wherein the steps of creating and ordering are executed automatically by a first process of the gateway machine and in that said first process generates a second process that executes the third and the fourth step.

12. (Previously Presented) A method according to claim 10, further comprising automatically executing the steps of creating, rerouting and deleting by a first process of the gateway machine and generating by said first process a second process that executes the steps of listening and generating a thread.

13. (Previously Presented) A method according to claim 11, further comprising automatically executing the steps of creating, rerouting and deleting by a first process of the gateway machine and generating by said first process a second process that executes the steps of listening and generating a thread.

14. (Currently Amended) A method for allowing a client application to establish in a client network a first connection having a first security level, with a first port of a server application hosted in a server machine linked to a server network, in order to send messages addressed to the server machine, said messages passing from the client network to the server network through a network layer (CR) of a gateway machine, characterized in that it consists of activating, in the gateway machine, a secure application proxy that reroutes the messages addressed to the first port of the server application away from the first connection, in a way that is transparent for the client application, in order to establish a second connection having a second security level with the server application, said second connection being unknown to said client application.